The SSHbase Plugin

SSHbase is a purpose build bcfg2 plugin for managing ssh host keys. It is responsible for making ssh keys persist beyond a client rebuild and building a proper ssh_known_hosts file, including a correct localhost record for the current system.

It has two functions:

- Generating new ssh keys -- When a client requests a dsa, rsa, or v1 key, and there is no existing key in the repository, one is generated.
- Maintaining the ssh_known_hosts file -- all current known public keys (and extra public key stores) are integrated into a single ssh_known_hosts file, and a localhost record for the current client is added. The ssh_known_hosts file data is updated whenever any keys change, are added, or deleted.

Interacting with SSHbase

- Pre-seeding with existing keys -- Currently existing keys will be overwritten by new, sshbase-managed ones by default. Pre-existing keys can be added to the repository by putting them in <repo>/SSHbase/<key filename>.H_<hostname>
- Pre-seeding can also be performed using bcfg2-admin pull ConfigFile /name/of/ssh/key
- Revoking existing keys -- deleting <repo>/SSHbase/*.H_<hostname> will remove keys for an existing client.

Getting started

1. Add SSHbase to the generators line in /etc/bcfg2.conf and restart the server -- This enables the SSHbase plugin in the bcfg2 server.
2. Add ConfigFile entries for /etc/ssh/ssh_known_hosts, and /etc/ssh/ssh_host_dsa_key, etc to a bundle or base.
3. Enjoy.

At this point, SSHbase will generate new keys for any client without a recorded key in the repository, and will generate an ssh_known_hosts file appropriately.

Blog post

http://www.ducea.com/2008/08/24/using-the-bcfg2-sshbase-plugin/